IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Xiang	
Application No.: 10/611392	Group Art Unit: 2416
Filed: 6/30/2003	Examiner: Patel
Title: A Method for Maintaining Data Flow in a Network Device Combining Diffserv and IPSEC Protocols	Confirmation No.: 1535
Attorney Docket No.: 120-038	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Please enter this Appeal Brief and contemporaneously filed Notice of Appeal.

I. Real Party in Interest

The real party in interest is Nortel Networks Limited.

II. Related Appeals and Interferences

Appellants are not aware of any related appeals or interferences.

III. Status of the Claims

Claims 2-5, 7-9 and 13-18 are currently pending in this application. All of the pending claims are rejected. No claims have been allowed. The status of claims 2-5, 7-9 and 13-18 is "previously presented." Claims 1, 6 and 13-18 have been cancelled. The rejections of independent claims 2, 13 and 18 are the subject of this appeal.

IV. Status of Amendments

All submitted amendments have been entered and considered.

V. Summary of Claimed Subject Matter

The present invention concerns supporting quality of service (QoS) in a secure network environment. One aspect of providing a secure network environment is use of a protocol such as IPSec that helps to protect against attacks. IPsec includes an Authentication Header (AH) that provides connectionless integrity and data origin authentication for IP datagrams, and protects against replays. Anti-replay helps to counter denial of service (DoS)

attacks which operate by flooding a network with redundant traffic. The IPSec anti-replay mechanism helps to thwart DoS attacks by comparing the sequence numbers of received packets and dropping any packets having duplicate sequence numbers within a predefined window of time. However, sequence numbers are not globally unique, and may be legitimately duplicated for traffic associated with different streams. Consequently, legitimate traffic may be dropped by the anti-replay mechanism. The presently recited invention changes the susceptibility of legitimate traffic to drop by the anti-replay mechanism on the basis of quality of service level. The specific tool used to implement the functionality is the anti-replay look back window in which sequence numbers are compared. For example, higher priority traffic may be filtered using a *smaller* anti-replay lookback window than lower priority traffic. An extreme example would be a window of size zero for the highest priority traffic, which would effectively exempt that traffic from drop by the anti-replay mechanism. It will be appreciated that this allows the network operator to balance network security against QoS traffic priority by, e.g., lowering network security in order to reduce the likelihood of inappropriate drop of higher priority traffic by the anti-replay mechanism.

The limitations recited in the independent claims are supported by the specification and drawing as indicated in **bold** below.

Claim 2. (previously presented) A method for determining whether to discard a received packet at a node, the method including the steps of:

establishing a first look-back window of a first size for packets associated with a first service level; **"Each Per Hop Behavior has a separate associated anti-replay bitmask, representing sequence numbers associated with the Per Hop Behavior that were received during a predetermined window, (such as a thirty two packet window). Each anti-replay bitmask is associated with a defined per hop Behavior aggregate, such as Best Effort (BE), one of a set of Assured Forwarding (AF) per hop behaviors, Expedited Forwarding (EF) or the like." Page 9:3-8.**

establishing a second look-back window of a second size for packets associated with a second service level, where the first look-back window is different than the second look-back window and the first size is different than the second size and the first service level is different than the second service level; **Id.**

comparing a sequence number associated with a first received packet against sequence numbers associated with a selected number of previously received packets in the first look-back window, the selected number determined by the first size, wherein the first received packet has a quality of service level associated therewith, the wherein the selected number of previously received packets are of the same quality of service level as the first received packet; **"When a packet is received at the node, the parser 52 strips the DSCP field and the sequence number from the respective IP and AH/ESP headers. The PSCP field is used to obtain a portion of the per hop behavior mapping information, which is forwarded to the packet processor. The packet**

processor retrieves the anti-replay bitmask for the PHB from the bitmask table 58. The packet processor compares the anti-replay bitmask, which incorporates the sequence numbers of previous packets received within the PHB window, to the current sequence number to find a match." Page 9:20-27.

comparing a sequence number associated with a second received packet against sequence numbers associated with a selected number of previously received packets in the second look-back window, the selected number determined by the second size, wherein the second received packet has a quality of service level associated therewith that differs from the first received packet, and wherein the selected number of previously received packets are of the same quality of service level as the second received packet, whereby the selected number of previously received packets examined in the step of comparing differs for at least two quality of service levels; **Id.**

discarding the first received packet in the event of a match between any one of the sequence numbers associated with the previously received packets in the first look-back window and the sequence number associated with the first received packet; and **"If a match is found within this window or the packet falls out of the PHB window, the current packet is discarded because it is a potential DoS attack. If no match is found, the packet is processed in accordance with the remaining fields of the IP header." Page 9:27-29.**

discarding the second received packet in the event of a match between any one of the sequence numbers associated with the previously received packets in

the second look-back window and the sequence number associated with the second received packet, **Id.**

whereby the number of sequence numbers compared with the sequence number of the first received packet differs from the number of sequence numbers compares with the sequence number of the second packet. **"PHBs of higher priority may have smaller anti-replay windows than those with higher priority." Page 11:5-6.**

Claims 13. (previously presented) An apparatus for discarding redundant packets received at a receiving node, comprising:

a sequence number buffer, for storing sequence numbers associated with packets received at the receiving node, wherein a packet is assigned a sequence number responsive to a quality of service level of the packet and a sequence number of a prior packet having the quality of service level of the packet; **"Each Per Hop Behavior has a separate associated anti-replay bitmask, representing sequence numbers associated with the Per Hop Behavior that were received during a predetermined window, (such as a thirty two packet window). Each anti-replay bitmask is associated with a defined per hop Behavior aggregate, such as Best Effort (BE), one of a set of Assured Forwarding (AF) per hop behaviors, Expedited Forwarding (EF) or the like." Page 9:3-8.**

a first look-back window of a first size for packets associated with a first service level; a second look-back window of a second size for packets associated

with a second service level, wherein the first look-back window is different than the second look-back window and the first size is different than the second size and the first service level is different than the second service level; **"PHBs of higher priority may have smaller anti-replay windows than those with higher priority." Page 11:5-6.**

an anti-replay bitmask table including a first entry associated with the first look-back window and a second entry associated with the second look-back window, each entry associated with a different quality of service level and storing the bitmask of sequence numbers of previously received packets to be compared in determining whether to discard a received packet, wherein a number of sequence numbers of previously received packets that are compared differs for at least two quality of service levels because the first size is different than the second size. **"When a packet is received at the node, the parser 52 strips the DSCP field and the sequence number from the respective IP and AH/ESP headers. The PSCP field is used to obtain a portion of the per hop behavior mapping information, which is forwarded to the packet processor. The packet processor retrieves the anti-replay bitmask for the PHB from the bitmask table 58. The packet processor compares the anti-replay bitmask, which incorporates the sequence numbers of previous packets received within the PHB window, to the current sequence number to find a match." Page 9:20-27.**

18. (previously presented) An apparatus comprising:

means for receiving a plurality of packets having an associated plurality of sequence numbers, wherein each one of the packets in the plurality of packets has a quality of service level associated therewith, and wherein there are at least two types of service levels; **"Referring now to Figure 4, some basic components of a networked node 50 are shown to include a packet processor 56, a parser 52 and a packet buffer 54. Although the components are shown as functional blocks, it should be understood that the functionality described with regard to each of the components may be implemented in either software, hardware, or a combination thereof, and the present invention is not limited to any specific implementation. Page 8:5-9. Each Per Hop Behavior has a separate associated anti-replay bitmask, representing sequence numbers associated with the Per Hop Behavior that were received during a predetermined window, (such as a thirty two packet window). Each anti-replay bitmask is associated with a defined per hop Behavior aggregate, such as Best Effort (BE), one of a set of Assured Forwarding (AF) per hop behaviors, Expedited Forwarding (EF) or the like." Page 9:3-8.**

a first look-back window of a first size for packets associated with a first service level; a second look-back window of a second size for packets associated with a second service level, wherein the first look-back window is different than the second look-back window and the first size is different than the second size and the first service level is different than the second service level; **"PHBs of higher priority may have smaller anti-replay windows than those with higher priority." Page 11:5-6.**

means for comparing, for each received packet, a received sequence number of each received packet against a set of previously received sequence numbers, wherein the set of sequence numbers includes only sequence numbers of packets previously received within a look-back window associated with a quality of service level type corresponding to the quality of service level type of the received packet and wherein a number of previously received sequence numbers for each set differs for at least two quality of service levels because the first size is different than the second size; and **"When a packet is received at the node, the parser 52 strips the DSCP field and the sequence number from the respective IP and AH/ESP headers. The PSCP field is used to obtain a portion of the per hop behavior mapping information, which is forwarded to the packet processor. The packet processor retrieves the anti-replay bitmask for the PHB from the bitmask table 58. The packet processor compares the anti-replay bitmask, which incorporates the sequence numbers of previous packets received within the PHB window, to the current sequence number to find a match." Page 9:20-27.**

means for discarding the received packet in the event of a match between the received sequence number and any of the sequence numbers in the set of sequence numbers in the look-back window of the same quality of service level type. **"If a match is found within this window or the packet falls out of the PHB window, the current packet is discarded because it is a potential DoS attack. If no match is found, the packet is processed in accordance with the remaining fields of the IP header." Page 9:27-29.**

VI. Grounds of Rejection to be Reviewed on Appeal

A. Claims 2, 3, 13, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 7,260,392 (Kitchin) in view of US 6,839,327 (Zavalkovsky).

B. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Zavalkovsky in view of US 7,099,327 (Nagarajan).

C. Claims 5, 7-9 and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kitchin in view of Zavalkovsky and US 7,020,143 (Zdan).

D. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kitchin in view of Zavalkovsky and US 7,000,120 (Koodli).

VII. Argument

A. The cited combination fails to teach or suggest all of the limitations recited in claims 2, 3, 13, and 18.

Three basic criteria must be met in order to establish a *prima facie* case of obviousness. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Third, the prior art references must teach or suggest all the claim limitations. (MPEP §2143)

The cited combination fails to teach or suggest all the claim limitations because the references do not describe different size anti-replay windows for different service levels as recited in independent claims 2, 13 and 18. The Office concedes that Kitchin fails to describe different size anti-replay windows for different service levels, but asserts that the feature is shown by buffer factor field 226 in figure 2 of Zavalkovsky. The buffer factor field is described in Zavalkovsky at column 8, lines 50 through 60 as follows:

> The value of Buffer Factor field 226 defines a percentage of the buffer resources that are allocated for the behavior aggregate. This is an alternative representation of the Reserved Packets field 224. It allows the network administrator to manage its buffer resources without knowledge of the particular queue lengths. In order to translate the buffer factor field into an Actual Reserved Packet field, a global parameter specifying the total buffer space should be used. The sum of buffer factors assigned to the forwarding classes is 100%. Within each forwarding class, **the buffer factor specifies the relative drop precedence of the PHBs.** (emphasis added)

As previously stated by appellant, unlike the buffer factor field 226, the anti-replay windows recited in the claims do not specify packet drop precedence,

do not specify a percentage, and do not add up to 100%. Therefore, the features are not equivalent.

Appellant respectfully suggests that the arguments advanced in favor of allowance have been misunderstood, as evidenced by the examiner's focus on the fact that both the recited invention and Zavalkovsky help to manage resource usage. Numerous and varied techniques for managing resources are known in the prior art, but appellant does not claim to have invented resource management in general, or even buffer allocation, sliding windows or the other specific tools that can be used to implement resource management. Many techniques for management of resources, at least some of which are patented, are based on different applications of the same set of basic tools to provide preferential treatment of particular traffic. The application of tools which distinguishes the pending claims is use of different size anti-replay look back windows for different service levels. An advantage of this, as described in the summary section above, is that security can be reduced for higher priority traffic in order to reduce the susceptibility of that traffic to being dropped by the anti-replay mechanism due to a misdiagnosis of a DoS attack. The combination of Kitchin and Zavalkovsky fails to produce that feature because packet drop precedence is not related to anti-replay look back window size or diagnosing DoS attacks. Packet drop precedence determines which packets are dropped in the event of *congestion*, whereas the anti-replay look back window size determines how many previous packets are compared with a current packet to test for repeated sequence numbers. Consequently,

combining the buffer factor field 226 of Zavalkovsky would not alter any anti-replay feature of Kitchin or yield the recited invention.

In the "response to arguments" at page 2 of the final office action the examiner asserts that Zavalkovsky teaches different "buffer factors" for different service levels, and that the "buffer factors" are the same as look back windows. Appellant respectfully submits that the buffer factors are not the same as look back windows for the following reasons:

(1) the buffer factor specifies the *%* of a buffer allocated to storing packets of *a forwarding class*, whereas the look back window specifies the *number* of previously received packets of *all classes* that are compared to find duplicate sequence numbers;

(2) the buffer factor results in preferential storage of a forwarding class only *when a node is congested*, whereas the different size look back windows result in preferential treatment of a particular QoS level *at all times*;

(3) the buffer factor trades off *storage* for *one forwarding class in favor of another forwarding class*, whereas the different size look back windows trade off *overall network security in favor of a particular QoS level*;

(4) the buffer factor has *no effect* on an anti-replay mechanism, whereas the the different size look back windows *directly affect* the anti-replay mechanism;

(5) the buffer factor *limits the bandwidth* available to a forwarding class, whereas the different size look back windows have *no effect on bandwidth*.

B. Claim 4 is allowable for the same reasons as claim 2.

If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

C. Claims 5, 7-9 and 14-16 are allowable for the same reasons as their respective base claims.

If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *Id.*

D. Claim 17 is allowable for the same reasons ass claim 13.

If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *Id.*

Conclusion

The rejections are improper for at least the reasons set forth above. Appellants accordingly request that the rejections be reversed and the application put forward for allowance.

Respectfully submitted,

/Holmes W. Anderson/
Holmes W. Anderson
Reg. No. 37,272
Attorney for Assignee

Date: November 16, 2009

Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton MA 01720
(978) 264-4001

Appendix A - Claims

1. (cancelled)

2. (previously presented) A method for determining whether to discard a received packet at a node, the method including the steps of:

establishing a first look-back window of a first size for packets associated with a first service level;

establishing a second look-back window of a second size for packets associated with a second service level, where the first look-back window is different than the second look-back window and the first size is different than the second size and the first service level is different than the second service level;

comparing a sequence number associated with a first received packet against sequence numbers associated with a selected number of previously received packets in the first look-back window, the selected number determined by the first size, wherein the first received packet has a quality of service level associated therewith, the wherein the selected number of previously received packets are of the same quality of service level as the first received packet;

comparing a sequence number associated with a second received packet against sequence numbers associated with a selected number of previously received packets in the second look-back window, the selected number determined by the second size, wherein the second received packet has a quality of service level associated therewith that differs from the first received packet, and wherein the selected number of previously received packets are of the same quality of service level as the second received packet, whereby the selected number of previously received packets examined in the step of comparing differs for at least two quality of service levels;

discarding the first received packet in the event of a match between any one of the sequence numbers associated with the previously received packets in the first look-back window and the sequence number associated with the first received packet; and

discarding the second received packet in the event of a match between any one of the sequence numbers associated with the previously received packets in the second look-back window and the sequence number associated with the second received packet,

whereby the number of sequence numbers compared with the sequence number of the first received packet differs from the number of sequence numbers compares with the sequence number of the second packet.

3. (previously presented) The method according to claim 2, further comprising forwarding the received packet for processing in the event that there is no match between any one of the sequence numbers associated with the selected number of previously received packets having the same quality of service as the received packet and the sequence number of the received packet.

4. (previously presented) The method according to claim 2 further comprising forwarding the received packet for processing in the event that the received packet is received a predetermined time after the selected number of previously received packets.

5. (previously presented) The method of claim 2, wherein the quality of service level is determined in response to a differentiated services codepoint (DSCP) associated with the packet.

6. (cancelled)

7. (previously presented) The method according to claim 3, wherein at least one of the quality of service levels corresponds to an Expedited Forwarding (EP) per hop behavior.

8. (previously presented) The method according to claim 3, wherein at least one of the quality of service levels corresponds to an Assured Forwarding (AF) per hop behavior.

9. (previously presented) The method according to claim 3, wherein at least one of the quality of service levels corresponds to a Best Efforts (BE) per hop behavior.

10. (cancelled)

11. (cancelled)

12. (cancelled)

13. (previously presented) An apparatus for discarding redundant packets received at a receiving node, comprising:

a sequence number buffer, for storing sequence numbers associated with packets received at the receiving node, wherein a packet is assigned a sequence number responsive to a quality of service level of the packet and a sequence number of a prior packet having the quality of service level of the packet;

a first look-back window of a first size for packets associated with a first service level;

a second look-back window of a second size for packets associated with a second service level,

wherein the first look-back window is different than the second look-back window and the first size is different than the second size and the first service level is different than the second service level;

an anti-replay bitmask table including a first entry associated with the first look-back window and a second entry associated with the second look-back window, each entry associated with a different quality of service level and storing the bitmask of sequence numbers of previously received packets to be compared in determining whether to discard a received packet, wherein a number of sequence numbers of previously received packets that are compared differs for at least two quality of service levels because the first size is different than the second size.

14. (previously presented) The apparatus of claim 13, wherein one of the entries of the anti-replay bitmask table is associated with an Expedited Forwarding (EF) service level.

15. (previously presented)The apparatus of claim 13, wherein one of the entries of the anti-replay bitmask table is associated with an Assured Forwarding (AF) service level.

16. (previously presented) The apparatus of claim 13, wherein one of the entries of the anti-replay bitmask table is associated with a Best Effort (BE) service level.

17. (previously presented) The apparatus of claim 13, wherein the apparatus operates according to an Internet Protocol Security (IPsec) protocol.

18. (previously presented) An apparatus comprising:

means for receiving a plurality of packets having an associated plurality of sequence numbers, wherein each one of the packets in the plurality of packets has a quality of service level associated therewith, and wherein there are at least two types of service levels;

a first look-back window of a first size for packets associated with a first service level;

a second look-back window of a second size for packets associated with a second service level,

wherein the first look-back window is different than the second look-back window and the first size is different than the second size and the first service level is different than the second service level;

means for comparing, for each received packet, a received sequence number of each received packet against a set of previously received sequence numbers, wherein the set of sequence numbers includes only sequence numbers of packets previously received within a look-back window associated with a quality of service level type corresponding to the quality of service level type of the received packet and wherein a number of previously received sequence numbers for each set differs for at least two quality of service levels because the first size is different than the second size; and

means for discarding the received packet in the event of a match between the received sequence number and any of the sequence numbers in the set of sequence numbers in the look-back window of the same quality of service level type.

Appendix B - Evidence Submitted

None.

Appendix C - Related Proceedings

None.